UNITED STATES DISTRICT COURT

for the

District of Oregon

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Apple iPhone 5S cellular telephone, model number A1453, with serial number 352029066888465, located at 1201 NE Lloyd Blvd, Suite 600, Portland, Oregon

Case No. 3:20-mc-00676

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Apple iPhone 5S cellular telephone, model number A1453, with serial number 352029066888465, currently located at 1201 NE Lloyd Boulevard, Suite 600, Portland, Oregon 97232. as described in Attachment A hereto,

located in the _____ District of Oregon, there is now concealed *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC §§ 2251(a) & 2252A	Production of child pornography and transportation, distribution, receipt, and possession of child pornography.

The application is based on these facts:

See affidavit which is attached hereto and incorporated herein by this reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Miguel A. Perez, Special Agent, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone at 10:20am. *(specify reliable electronic means).*

Date: 07/08/2020

Jolie A Russo
Judge's signature

City and state: Portland, Oregon

Honorable Jolie A. Russo, United States Magistrate Judge
Printed name and title

ATTACHMENT A

Property to Be Searched

The property to be searched is an Apple iPhone 5S cellular telephone, model number A1453, with serial number 352029066888465 and is currently located on the premises of the Northwest Regional Computer Forensics Laboratory (NWRCFL) located at 1201 NE Lloyd Boulevard, Suite 600, Portland, Oregon 97232.

ATTACHMENT B

Items to Be Seized

1. All records on the Device described in Attachment A that relate to violations of Title 18, United States Code, §§ 2251(a) and 2252A, involving the production of child pornography and transportation, distribution, receipt, and possession of child pornography, and involves Andrew Thomas Tager since June 1, 2015, including:

a. Any and all records, documents, or materials, including correspondence, that pertain to the production, possession, receipt, transportation, or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in as defined in Title 18, United States Code, Section 2256.

b. All originals and copies of visual depictions of minors engaged in sexually explicit conduct, as defined in as defined in Title 18, United States Code, Section 2256.

c. Any and all motion pictures or digital video clips of visual depictions of minors engaged in sexually explicit conduct, as defined in as defined in Title 18, United States Code, Section 2256, video recordings which are self-produced and pertain to sexually explicit images of minors; or video recordings of minors which may assist in the location of minor victims of child exploitation or child abuse;

d. Any and all records, documents, or materials which include offers to transmit, through interstate commerce by any means, any visual depiction of a minor engaged in sexually explicit conduct, as defined in as defined in Title 18, United States Code, Section 2256.

e. Any and all records, documents, or materials relating to the production,

reproduction, receipt, shipment, trades, purchases, or transactions of any kind involving the transmission, through interstate commerce, of any visual depiction of a minor engaged in sexually explicit conduct, as defined in as defined in Title 18, United States Code, Section 2256.

f. Any and all records, documents, or materials naming or identifying minors visually depicted while engaging in sexually explicit conduct, as defined in as defined in Title 18, United States Code, Section 2256.

g. Any records of Internet usage, including records containing screen names, user names, and e-mail addresses, and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, and e-mail messages.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. Records evidencing the use of the Internet, including:

a. Records of Internet Protocol addresses used.

b. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

c. Records of data storage accounts and use of data storage accounts.

4. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or

stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

Search Procedure

5. The examination of the Device may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

6. The initial examination of the Device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

7. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Device or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

8. If an examination is conducted, and it is determined that the Device does not

contain any data falling within the ambit of the warrant, the government will return the Device to its owner within a reasonable period of time following the search and will seal any image of the Device, absent further authorization from the Court.

9. The government may retain the Device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Device and/or the data contained therein.

10. The government will retain a forensic image of the Device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

DISTRICT OF OREGON, ss: AFFIDAVIT OF MIGUEL A. PEREZ

Affidavit in Support of an Application Under Rule 41 for a Warrant to Search and Seize Evidence Including Digital Evidence

I, Miguel A. Perez, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been since January 2015. I am currently assigned to the Portland Division at the Eugene, Oregon Resident Agency. During my training at the FBI Academy in Quantico, Virginia, I received training in a variety of investigative and legal matters, including the topics of Fourth Amendment Searches and probable cause. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2252A, and I am authorized by the Attorney General to request a search warrant.

2. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search and examination of an **Apple iPhone 5S** cellular telephone, model number **A1453**, with serial number **352029066888465**, (hereinafter "Device"), which is currently stored, in law enforcement possession, on the premises of the Northwest Regional Computer Forensics Laboratory (NWRCFL) located at 1201 NE Lloyd Boulevard, Suite 600, Portland, Oregon 97232, as described in Attachment A hereto, and the extraction of electronically stored information from the Device, as described in Attachment B hereto. As set forth below, I have probable cause to believe and do believe that the items set forth in Attachment B constitute evidence of contraband, fruits, and instrumentalities of violations of Title 18, United States Code, §§ 2251(a) and 2252A,

involving the production of child pornography and transportation, distribution, receipt, and possession of child pornography.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Applicable Law

4. Title 18, U.S.C., § 2251(a) makes it a crime to knowingly employ, use, persuade, induce, entice, or coerce a minor to engage in sexually explicit conduct for the purpose of producing a visual depiction of that conduct, if the person knows or has reason to know that the visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce if the visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or if it was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer.

5. Title 18, United States Code, Section § 2252A (a)(1) makes it a crime to knowingly transport child pornography using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means, including by

computer. Section 2252A(a)(2) makes it a crime to knowingly receive or distribute any child pornography that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means or facility, including by computer. Title 18, United States Code, Section 2252A(a)(5)(B) makes it a crime to knowingly possess or access with intent to view child pornography that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that were mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer. The term child pornography is defined in Title 18, United States Code, Section 2256(8).

Child Pornography

6. I know, based on my training and experience, and based on conversations I have had with others who investigate child exploitation offenses, that people who have a sexual interest in children, including people who collect and trade in child pornography, often receive sexual gratification from images and video clips depicting the sexual exploitation of children. They may also use such images and videos to lower the inhibitions of children who they wish to sexually abuse. Such people maintain their collections of child pornography in safe, secure, and private locations, such as their residence, and on computers and digital storage media under their direct control. Such people often maintain their collections, which are considered prized possessions, for long periods of time, and prefer not to be without their collections for any prolonged period of time.

/ / / /

/ / / /

Previous Warrants Authorized

7. The court previously authorized the following warrants in this matter:

a) On March 13, 2019, the court authorized a search warrant for information associated with TikTok account "cherokeetager", stored by TikTok.com. Case No. 6:19-mc-223.

b) On March 13, 2019, the court authorized a search warrant for information associated with Snapchat account "cherokeetager", stored by Snapchat, Inc. Case No. 6:19-mc-224.

c) On March 13, 2019, the court authorized a search warrant for information associated with Instagram account "atagerofficial", stored by Facebook, Inc. Case No. 6:19-mc-221.

d) On March 13, 2019, the court authorized a search warrant for information associated with email account "jessicamillsmoderator@outlook.com", stored by Microsoft Corporation. Case No. 6:19-mc-220. On April 3, 2019, the search warrant was Amended, Case No. 6:19-mc-220 Amended.

e) On March 13, 2019, the court authorized a search warrant for information associated with email accounts tagerdude24@gmail.com, tagerdude25@gmail.com, and tagerdude28@gmail.com, stored at Google LLC. Case No. 6:19-mc-222. On April 3, 2019, the search warrant was Amended, Case No. 6:19-mc-222 Amended.

f) On May 2, 2019, the court authorized a search warrant for information associated with cellular telephone assigned call number (336) 314-6434

whose wireless service provider was Verizon Wireless. Case No. 6:19-mc-389.

g) On May 2, 2019, the court authorized an arrest warrant for **Andrew Thomas Tager** pursuant to a criminal complaint in violation of Title 18, United States Code, § 2251(a), involving the production of child pornography, and Title 18, United States Code, § 2252A, involving the transportation, receipt, and possession of child pornography.

h) On June 18, 2019, the court authorized a search warrant for information associated with the account tagerdude24@gmail.com account stored at Dropbox, Inc. Case No. 6:19-mc-517.

i) On June 18, 2019, the court authorized a search warrant for digital devices related to **Tager** Investigation located in law enforcement custody at FBI Eugene. Case No. 6:19-mc-518.

j) On January 10, 2020, the court authorized a search warrant for the same Device described in this warrant, which was in law enforcement custody at FBI Portland. Case No. 6:20-mc-30.

Statement of Probable Cause

8. I have been involved and continue to be involved in an investigation of **Tager** for activities related to the production and possession of child pornography. I believed **Tager** was in violation for the productions of child pornography and transportation, receipt, and possession of child pornography. An arrest warrant was granted on May 2, 2019 and on May 30, 2019 **Tager** was arrested pursuant to the arrested warrant.

9. As described more fully in the affidavit in support of the search warrant listed in paragraph 7(j) for the Device, I had probable cause to believe and do believe that the Device held evidence of contraband, fruits, and instrumentalities of violations of Title 18, United States Code, §§ 2251(a) and 2252A, involving the production of child pornography and transportation, distribution, receipt, and possession of child pornography. The search warrant in paragraph 7(j) is attached and incorporated as Exhibit A.

10. As described in Exhibit A, on November 12, 2019, **Tager's** girlfriend, now ex-girlfriend (EGF), contacted me and informed me she had found an iPhone that belonged to **Tager**. On November 13, 2019, EGF gave the phone to an Agent in Greensboro, North Carolina. On November 25, 2019, the phone was shipped by FedEx to the Portland FBI office and arrived the following day.

11. On January 10, 2020, the court granted the search warrant attached as Exhibit A. I then submitted the Device to the NWRCFL for the digital forensic examination. A Digital Forensic Examiner took steps to make information on the Device available for the examination of digital evidence. The Device also required a four-digit passcode to access its contents. A Digital Forensic Examiner used methods to break the passcode. On April 24, 2020, the Digital Forensic Examiner broke the passcode and did a data pull of the Device. The initial examination of the contents pulled from the Device was not performed within the 120 days from the execution of the warrant as stated in Attachment B of Exhibit A. Therefore, I am requesting a new warrant authorizing the examination of the contents of the Device.

12. The Device is currently in the lawful possession of the FBI. The Device is currently stored at the offices of the NWRCFL located at 1201 NE Lloyd Boulevard, Suite 600,

Portland, Oregon 97232. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the Portland FBI.

13. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. *Wireless telephone*. A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. *Digital camera*. A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage

medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. *Portable media player*. A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. *GPS*. A GPS navigation device uses the Global Positioning System to display its current location. It often contains historical records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated as "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude

with a high level of precision.

e. *PDA*. A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments, or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive email. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. *Storage medium*. A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

g. *IP address*. An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. *Internet*. The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet,

connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

14. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, storage medium, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

15. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

16. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence will be on the Device because, based on my knowledge, training, and experience, I know:

a. Data on the Device can provide evidence of a file that was once on the Device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of

occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the device at a relevant time. Further, forensic evidence on a device can show how and when the device was accessed or used. Such "timeline" information allows the forensic analyst and investigators to understand the chronological context of access, use, and events relating to the crime under investigation. This "timeline" information may tend to either inculpate or exculpate the device user. Last, forensic evidence on a device may provide relevant insight into the device user's state of mind as it relates to the offense under investigation. For example, information on a device may indicate the user's motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a "wiping program" to destroy evidence on the device or password protecting or encrypting such evidence in an effort to conceal it from law enforcement), or knowledge that certain information is stored on a computer (e.g., logs indicating that the incriminating information was accessed with a particular program).

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to

investigators. Whether data stored on a device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

17. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

18. The initial examination of the Device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

19. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Device or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

20. If an examination is conducted, and it is determined that the Device does not contain any data falling within the ambit of the warrant, the government will return the Device to its owner within a reasonable period of time following the search and will seal any image of the Device, absent further authorization from the Court.

21. The government may retain the Device as evidence, fruits, contraband, or an instrumentality of a crime, or to commence forfeiture proceedings against the Device and/or the data contained therein.

22. The government will retain a forensic image of the Device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

23. *Manner of execution*. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve

the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Conclusion

24. Based on the foregoing, I have probable cause to believe, and I do believe, that the Device described in Attachment A contains evidence of contraband, fruits, and instrumentalities of violations of Title 18, United States Code, §§ 2251(a) and 2252A, involving the production of child pornography and transportation, distribution, receipt, and possession of child pornography, as set forth in Attachment B. I therefore request that the Court issue a warrant authorizing a search of the Device described in Attachment A for the items listed in Attachment B and the seizure and examination of any such items found.

25. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) Ashley Cadotte advised me that in her opinion the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

By Phone
Miguel A. Perez
Special Agent
Federal Bureau of Investigation

Sworn in before me in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone at 10:20 a.m on July _8__, 2020.

Jolie A Russo
HONORABLE JOLIE A. RUSSO
United States Magistrate Judge

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of Oregon

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Apple iPhone 5S cellular telephone, model number A1453, with serial number 352029066888465, currently located at 9109 NE Cascades Pkwy, Portland, OR 97220

Case No. 6:20-mc-30

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Apple iPhone 5S cellular telephone, model number A1453, with serial number 352029066888465, currently located at 9109 NE Cascades Pkwy, Portland, OR 97220 as described in Attachment A hereto,

located in the _____ District of Oregon, there is now concealed *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC §§ 2251(a) & 2252A	Production of child pornography and transportation, distribution, receipt, and possession of child pornography.

The application is based on these facts:
See affidavit which is attached hereto and incorporated herein by this reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Miguel A. Perez
Applicant's signature

Miguel A. Perez, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 1/10/2020

Judge's signature

City and state: Eugene, Oregon

Mustafa T. Kasubhai, United States Magistrate Judge
Printed name and title

DISTRICT OF OREGON, ss: AFFIDAVIT OF MIGUEL A. PEREZ

Affidavit in Support of an Application Under Rule 41 for a Warrant to Search and Seize Evidence Including Digital Evidence

I, Miguel A. Perez, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been since January 2015. I am currently assigned to the Portland Division at the Eugene, Oregon Resident Agency. During my training in the FBI Academy in Quantico, Virginia, I received training in a variety of investigative and legal matters, including the topics of Fourth Amendment Searches and probable cause. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2252A, and I am authorized by the Attorney General to request a search warrant.

2. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search and examination of an **Apple iPhone 5S** cellular telephone, model number **A1453**, with serial number **352029066888465**, (hereinafter "Device"), which is currently stored, in law enforcement possession, on the premises of the Federal Bureau of Investigation at 9109 NE Cascades Parkway, Portland, Oregon 97220, as described in Attachment A hereto, and the extraction of electronically stored information from the Device, as described in Attachment B hereto. As set forth below, I have probable cause to believe and do believe that the items set forth in Attachment B constitute evidence of contraband, fruits, and instrumentalities of violations of Title 18, United States Code, §§ 2251(a) and 2252A, involving the production of child pornography and transportation, distribution, receipt, and possession of child pornography.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Applicable Law

4. Title 18, U.S.C., § 2251(a) makes it a crime to knowingly employ, use, persuade, induce, entice, or coerce a minor to engage in sexually explicit conduct for the purpose of producing a visual depiction of that conduct, if the person knows or has reason to know that the visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce if the visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or if it was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer.

5. Title 18, United States Code, Section § 2252A (a)(1) makes it a crime to knowingly transport child pornography using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means, including by computer. Section 2252A(a)(2) makes it a crime to knowingly receive or distribute any child pornography that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means or facility, including by computer. Title 18, United States Code,

Section 2252A(a)(5)(B) makes it a crime to knowingly possess or access with intent to view child pornography that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that were mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer. The term child pornography is defined in Title 18, United States Code, Section 2256(8).

Child Pornography

6. I know, based on my training and experience, and based on conversations I have had with others who investigate child exploitation offenses, that people who have a sexual interest in children, including people who collect and trade in child pornography, often receive sexual gratification from images and video clips depicting the sexual exploitation of children. They may also use such images and videos to lower the inhibitions of children who they wish to sexually abuse. Such people maintain their collections of child pornography in safe, secure, and private locations, such as their residence, and on computers and digital storage media under their direct control. Such people often maintain their collections, which are considered prized possessions, for long periods of time, and prefer not to be without their collections for any prolonged period of time.

Previous Warrants Authorized

7. The court previously authorized the following warrants in this matter:

a) On March 13, 2019, the court authorized a search warrant for information associated with TikTok account "cherokeetager", stored by TikTok.com. Case No. 6:19-mc-223.

b) On March 13, 2019, the court authorized a search warrant for information associated with Snapchat account "cherokeetager", stored by Snapchat, Inc. Case No. 6:19-mc-224.

c) On March 13, 2019, the court authorized a search warrant for information associated with Instagram account "atagerofficial", stored by Facebook, Inc. Case No. 6:19-mc-221.

d) On March 13, 2019, the court authorized a search warrant for information associated with email account "jessicamillsmoderator@outlook.com", stored by Microsoft Corporation. Case No. 6:19-mc-220. On April 3, 2019, the search warrant was Amended, Case No. 6:19-mc-220 Amended.

e) On March 13, 2019, the court authorized a search warrant for information associated with email accounts tagerdude24@gmail.com, tagerdude25@gmail.com, and tagerdude28@gmail.com, stored at Google LLC. Case No. 6:19-mc-222. On April 3, 2019, the search warrant was Amended, Case No. 6:19-mc-222 Amended.

f) On May 2, 2019, the court authorized a search warrant for information associated with cellular telephone assigned call number (336) 314-6434 whose wireless service provider was Verizon Wireless. Case No. 6:19-mc-389.

g) On May 2, 2019, the court authorized an arrest warrant for **Andrew Thomas Tager** pursuant to a criminal complaint in violation of Title 18, United States Code, § 2251(a), involving the production of child

pornography, and Title 18, United States Code, § 2252A, involving the transportation, receipt, and possession of child pornography.

h) On June 18, 2019, the court authorized a search warrant for information associated with the account tagerdude24@gmail.com account stored at Dropbox, Inc. Case No. 6:19-mc-517.

i) On June 18, 2019, the court authorized a search warrant for digital devices related to **Tager** Investigation located in law enforcement custody at FBI Eugene. Case No. 6:19-mc-518.

Statement of Probable Cause

8. I have been involved and continue to be involved in an investigation of **Tager** for activities related to the production and possession of child pornography.

9. As described more fully in the affidavit in support of the criminal complaint arrest warrant for **Tager**, I believed **Tager** was in violation for the productions of child pornography and transportation, receipt, and possession of child pornography. The affidavit in support of the criminal complaint and arrest warrant, which was granted on May 2, 2019, is attached hereto and incorporated as Exhibit 1.

Introduction

10. As detailed in Exhibit 1, my investigation has revealed that, communicating over Kik Messenger (an online messaging platform), an individual—who I believe to be **Tager**—contacted at least one minor female (V1) and directed her to produce and send him pornographic pictures and videos through Kik Messenger. Many of the instructions to V1, which I believe were made while **Tager** was posing as an employee of the social media platform Musical.ly

(now known as TikTok)—and using, notably, the username "**Officalcrowns**" on Kik Messenger—included explicit direction on how V1 should pose, move, what she should wear, what props she should use, and how long the videos needed to be in the pornographic photographs and videos. I believe that **Tager** told V1 to participate in a fictional "Crown Program" and told her that, by sending the pictures and videos, she could earn a "Crown". He later told V1 that if she quit the program, her videos would bet released and people could go and subscribe to view her gallery of photos and videos.

11. The investigation has linked the **Officialcrowns** username to email addresses, tagerdude24@gmail.com and tagerdude25@gmail.com. For one thing, tagerdude25@gmail.com contains emails in which the account user tells an adult female that she can contact him on his Kik account, "**Officialcrowns**"---which is the same Kik account that **Officialcrowns** used to communicate with V1. Additionally, the two accounts, tagerdude24@gmail.com and tagerdude25@gmail.com, exchange emails containing child pornography, discussing whether a minor victim had earned a "Crown" and containing a list of things the victim needed to do—including needing to improve her ability to listen and follow instructions from Musical.ly and her Moderator "Musicalcrownpage". The email accounts appeared to indicate that the account user was employing multiple aliases, email accounts, and personas and that he is transferring child pornography and information between the email accounts by sending emails from one account to another. I know, from my training and experience as well as my conversations with other law enforcement officials, that people engaged in the online production of child pornography sometimes create multiple email and online accounts for themselves and others to use in storing information, transferring child pornography files, keeping track of their child exploitation efforts,

or, at times, communicating with other individuals who have been granted access to the accounts.

12. I also have a belief that **Tager** was actively involved in the sexual exploitation of children on Snapchat and Musical.ly was borne out by the discovery, through investigation, of TikTok (what Musical.ly is now called) and Snapchat accounts with the name **Cherokeetager**. Review of account records has revealed the **Cherokeetager** user posting a profile picture and videos that appear to be **Tager**, and discussing the "Crown Program" with girls between the ages of 10-12. His instructions to the minors are consistent with the discussion of the "Crown Program" that the user **Officialcrowns** employed in coercing V1 to produce and send child pornography.

Arrest of Tager

13. On May 30, 2019, at approximately 9:30 p.m., **Tager** was arrested by Special Agents of the FBI in Greensboro, North Carolina pursuant to the arrest warrant issued by the U.S. District Court for the District of Oregon on May 2, 2019. Tager asked for a lawyer after he was advised of his rights. Earlier in the day, the Agents had attempted to locate and arrest **Tager** at his residence and at his place of employment. The attempts to locate him were unsuccessful and **Tager's** girlfriend, other occupants of his apartment, and his work supervisor were aware the FBI was attempting to locate him. Several hours pasted between when the contacts were made and when **Tager** surrendered to the FBI.

Receipt of iPhone 5S

14. On November 12, 2019, **Tager's** girlfriend, now ex-girlfriend (AW1), contacted me and informed me she had found an iPhone that belonged to **Tager**. On November 13, 2019,

AW1 gave the phone to an Agent in Greensboro, North Carolina. On November 25, 2019, the phone was shipped by FedEx to the Portland FBI office and arrived the following day.

15. **Tager** lived with AW1 in her apartment at the time of his arrest. AW1 worked as a leasing agent for the apartment complex they lived at and is currently in the same position. The head of maintenance for the apartment complex found a cell phone on the property and took it into his office. AW1 walked into his office and AW1 recognized the phone as a cell phone, the Device, that belonged to **Tager**. AW1 was told the phone may have been found in some bushes. AW1 recognized the color, the markings, the damage, and the model of the phone. AW1 took possession the Device and contacted me as soon as she found it.

16. AW1 and **Tager** lived together for almost a year. **Tager** had the Device when he moved in with her. **Tager** eventually got a new phone but he kept the Device.

17. The Device is currently in the possession of the FBI. It came into the FBI's possession as described above. The Device is currently in storage at 9109 NE Cascades Parkway, Portland, Oregon 97220. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as it was when the Device first came into the possession of the FBI.

18. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. *Wireless telephone*. A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless

telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. *Digital camera*. A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. *Portable media player*. A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the

ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. *GPS*. A GPS navigation device uses the Global Positioning System to display its current location. It often contains historical records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated as "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. *PDA*. A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments, or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive email. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can

work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. *Storage medium*. A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

g. *IP address*. An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. *Internet*. The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

19. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, storage medium, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

20. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the

Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

21. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence will be on the Device because, based on my knowledge, training, and experience, I know:

a. Data on the Device can provide evidence of a file that was once on the Device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the device at a relevant time. Further, forensic evidence on a device can show how and when the device was accessed or used. Such "timeline" information allows the forensic analyst and investigators to understand the chronological context of access, use, and events relating to the crime under investigation. This "timeline" information may tend to either inculpate or exculpate the device user. Last, forensic evidence on a device may provide relevant

insight into the device user's state of mind as it relates to the offense under investigation. For example, information on a device may indicate the user's motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a "wiping program" to destroy evidence on the device or password protecting or encrypting such evidence in an effort to conceal it from law enforcement), or knowledge that certain information is stored on a computer (e.g., logs indicating that the incriminating information was accessed with a particular program).

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

22. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

23. The initial examination of the Device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

24. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Device or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

25. If an examination is conducted, and it is determined that the Device does not contain any data falling within the ambit of the warrant, the government will return the Device to

its owner within a reasonable period of time following the search and will seal any image of the Device, absent further authorization from the Court.

26. The government may retain the Device as evidence, fruits, contraband, or an instrumentality of a crime, or to commence forfeiture proceedings against the Device and/or the data contained therein.

27. The government will retain a forensic image of the Device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

28. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Conclusion

29. Based on the foregoing, I have probable cause to believe, and I do believe, that the Device described in Attachment A contains evidence of contraband, fruits, and instrumentalities of violations of Title 18, United States Code, §§ 2251(a) and 2252A, involving the production of child pornography and transportation, distribution, receipt, and possession of child pornography, as set forth in Attachment B. I therefore request that the Court issue a warrant authorizing a search of the Device described in Attachment A for the items listed in

Attachment B and the seizure and examination of any such items found.

30. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) Amy Potter advised me that in her opinion the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

Miguel A. Perez
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me this 10 day of January 2020.

Mustafa Kasubhai
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

The property to be searched is an Apple iPhone 5S cellular telephone, model number A1453, with serial number 352029066888465 and is currently located on the premises of the Federal Bureau of Investigation at 9109 NE Cascades Parkway, Portland, Oregon 97220.

ATTACHMENT B

Items to Be Seized

1. All records on the Device described in Attachment A that relate to violations of Title 18, United States Code, §§ 2251(a) and 2252A, involving the production of child pornography and transportation, distribution, receipt, and possession of child pornography, and involves Andrew Thomas Tager since June 1, 2015, including:

a. Any and all records, documents, or materials, including correspondence, that pertain to the production, possession, receipt, transportation, or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in as defined in Title 18, United States Code, Section 2256.

b. All originals and copies of visual depictions of minors engaged in sexually explicit conduct, as defined in as defined in Title 18, United States Code, Section 2256.

c. Any and all motion pictures or digital video clips of visual depictions of minors engaged in sexually explicit conduct, as defined in as defined in Title 18, United States Code, Section 2256, video recordings which are self-produced and pertain to sexually explicit images of minors; or video recordings of minors which may assist in the location of minor victims of child exploitation or child abuse;

d. Any and all records, documents, or materials which include offers to transmit, through interstate commerce by any means, any visual depiction of a minor engaged in sexually explicit conduct, as defined in as defined in Title 18, United States Code, Section 2256.

e. Any and all records, documents, or materials relating to the production,

reproduction, receipt, shipment, trades, purchases, or transactions of any kind involving the transmission, through interstate commerce, of any visual depiction of a minor engaged in sexually explicit conduct, as defined in as defined in Title 18, United States Code, Section 2256.

f. Any and all records, documents, or materials naming or identifying minors visually depicted while engaging in sexually explicit conduct, as defined in as defined in Title 18, United States Code, Section 2256.

g. Any records of Internet usage, including records containing screen names, user names, and e-mail addresses, and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, and e-mail messages..

Search Procedure

5. The examination of the Device may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

6. The initial examination of the Device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of

the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

7. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Device or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

8. If an examination is conducted, and it is determined that the Device does not contain any data falling within the ambit of the warrant, the government will return the Device to its owner within a reasonable period of time following the search and will seal any image of the Device, absent further authorization from the Court.

9. The government may retain the Device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Device and/or the data contained therein.

10. The government will retain a forensic image of the Device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

District of Oregon

United States of America
v.
Andrew Thomas Tager

Case No. 6:19-mj- 80-MK

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of May 2018 - Sept 2018 in the county of Coos in the District of Oregon, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. §§2251(a) and 2252A	Production of child pornography and transportation, receipt, and possession of child pornography

This criminal complaint is based on these facts:

The attached affidavit of SA Miguel A. Perez, which is incoporated herein

☑ Continued on the attached sheet.

Complainant's signature

Miguel A. Perez, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 5/2/19

Judge's signature

City and state: Eugene, Oregon

Thomas M. Coffin, U.S. Magistrate Judge

Printed name and title

GOVERNMENT EXHIBIT
Exhibit A
Page 22 of 46

DISTRICT OF OREGON, ss: AFFIDAVIT OF MIGUEL A. PEREZ

Affidavit in Support of a Criminal Complaint and Arrest Warrant

I, Miguel A. Perez, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been since January 2015. I am currently assigned to the Portland Division at the Eugene, Oregon Resident Agency. During my training in the FBI Academy in Quantico, Virginia, I received training in a variety of investigative and legal matters, including the topics of Fourth Amendment Searches and probable cause. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. § 2251, and I am authorized by the Attorney General to request a search warrant

3. This affidavit is made in support of a criminal complaint and arrest warrant for **Andrew Thomas Tager** (hereinafter "**Tager**"), for violation of Title 18, United States Code, § 2251(a), involving the production of child pornography, and Title 18, United States Code, § 2252A, involving the transportation, receipt, and possession of child pornography.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, investigators and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

Applicable Law

5. Title 18, U.S.C., § 2251(a) makes it a crime to knowingly employ, use, persuade, induce, entice, or coerce a minor to engage in sexually explicit conduct for the purpose of

producing a visual depiction of that conduct, if the person knows or has reason to know that the visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce if the visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or if it was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer.

6. Title 18, United States Code, Section § 2252A (a)(1) makes it a crime to knowingly transport child pornography using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means, including by computer. Section 2252A(a)(2) makes it a crime to knowingly receive or distribute any child pornography that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means or facility, including by computer. Title 18, United States Code, Section 2252A(a)(5)(B) makes it a crime to knowingly possess or access with intent to view child pornography that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that were mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer. The term child pornography is defined in Title 18, United States Code, Section 2256(8).

Statement of Probable Cause

7. As described more fully below, I believe that **Tager** produced and received child pornography in violation of federal law. My investigation has revealed that, communicating over Kik Messenger (an online messaging platform), an individual—who I believe to be **Tager**—contacted at

least one minor female (V1) and directed her to produce and send him pornographic pictures and videos through Kik Messenger. Many of the instructions to V1, which I believe were made while **Tager** was posing as an employee of the social media platform Musical.ly (now known as TikTok)—and using, notably, the username "**Officalcrowns**" on Kik Messenger—included explicit direction on how V1 should pose and move, what she should wear, what props she should use, and how long the videos needed to be. I believe that **Tager** told V1 to participate in a fictional "Crown Program" and told her that, by sending the pictures and videos, she could earn a "Crown". He later told V1 that if she quit the program, her videos would be released and people could go and subscribe to view her gallery of photos and videos.

8. The investigation has linked the **Officialcrowns** username to the following email addresses: tagerdude24@gmail.com, tagerdude25@gmail.com, tagerdude28@gmail.com, and jessicamillsmoderator@outlook.com. For example, tagerdude25@gmail.com contains emails in which the account user tells an adult female that she can contact him on his Kik account, "**Officialcrowns**"—which is the same Kik account that **Officialcrowns** used to communicate with V1. Additionally, the two accounts, tagerdude24@gmail.com and tagerdude25@gmail.com exchange emails containing child pornography, discussing whether a minor victim had earned a "Crown" and containing a list of things the victim needed to do—including needing to improve her ability to listen and follow instructions from Musical.ly and her moderator "Musicalcrownpage". The email accounts appear to indicate that the account user is employing multiple aliases, email accounts, and personas and that he is transferring child pornography and information between the email accounts by sending emails from one account to another. I know, from my training and experience as well as my conversations with other law enforcement officials, that people engaged in the online production of child pornography sometimes create

multiple email and online accounts for themselves and others to use in storing information, transferring child pornography files, keeping track of their child exploitation efforts, or, at times, communicating with other individuals who have been granted access to the accounts.

9. Based on the investigation, including the execution of search warrants on the email accounts, I believe that all the email accounts belong to **Tager**. For example, tagerdude24@gmail.com was found to contain an email addressed to **Andrew Tager** from **Tager**'s credit card company as well as emails with **Tager**'s resume and driver's license attached. Similarly, tagerdude25@gmail.com was found to contain an email in which an individual identifying himself as "**Andrew Tager**" sent someone a copy of **Andrew Tager**'s resume. The email stated that **Tager** is looking for a career in the gaming industry and is signed "Kind Regards, **Andrew Tager**." The resume included what I believe to be **Tager**'s correct phone number **(336) 314-6434**.

10. My belief that **Tager** is actively involved in the sexual exploitation of children on Snapchat and Musical.ly is borne out by the discovery, through investigation, of TikTok (what Musical.ly is now called) and Snapchat accounts with the name **Cherokeetager**. Review of account records has revealed the **Cherokeetager** user posting a profile picture and videos that appear to be **Tager**, and discussing the "Crown Program" with girls between the ages of 10-12. His instructions to the minors are consistent with the discussion of the "Crown Program" that the user Officialcrowns employed in coercing V1 to produce and send child pornography.

Identification of V1, Interview, and Review of Her Interactions with OfficialCrowns

11. On August 29, 2018, the FBI was contacted by the North Bend Police Department in Oregon about a case involving the online sexual corruption of a child. The parents reported that the Victim, V1, a ten year old female, whose identity is known to law enforcement, had been

sending nude photos and videos of herself using Kik to a person they believed was a male. The person, with username "**Officialcrowns**" on Kik, threatened that V1's photos would be released for other to views if she did not continue taking sexually explicit photos and recording videos of herself. V1 was told by the person she would earn "points" by doing as instructed until she reached a level where the images and recordings would not be released. The nature of the verbiage used by **Officialcrowns** with V1 was used in an effort to coerce her to comply with the demands. As a result, V1 complied with the demands and sent the pornographic material to **Officialcrowns** on Kik.

12. On September 4, 2018, V1 was interviewed by a child forensic interviewer in North Bend, Oregon. V1 disclosed that she had an account on Musical.ly. Musical.ly was a social media platform application on which users created and shared short videos. V1 was made aware of Musical.ly by her friend, a 10 year old female, (V2) whose identity is known to law enforcement. Her friend told V1 she could obtain "Crowns" to get access and privileges that were not available to everyone on the application. V1 started talking to a female who identified herself as "Dianna" on the **Officialcrowns** Kik account. V1 stated "Dianna" (hereinafter "**Officialcrowns**") said she worked for Muscial.ly and had access to V1's private account. **Officialcrowns** told V1 if she wanted a crown she had to do certain things to acquire the crown. V1 stated she did not care about having the crown, but was more concerned with protecting the content on her private Musical.ly account.

13. The FBI received consent from the parents of V1 to take possession of her IPod and to review its contents. A review of the Kik conversations between **Officialcrowns** and V1 appear to begin on or about May 15, 2018. V1 sent **Officialcrowns** several pornographic files on Kik, the following is some of what was discussed and shared:

a. The review revealed on or about June 17, 2018, **Officialcrowns** told V1 on Kik that her name was "Dianna". **Officialcrowns** told V1 that once she quit the program, her videos got released to their website. There people can go and subscribe to view her gallery of photos and videos. The only way to lock it down so nobody can subscribe and get her contact information on Muscal.ly was to get back in the program and staying active to finish. This would lock down V1's photos.

b. Later on, **Officialcrowns** sent V1 an image and asked her if she can get a "handle" like this one. V1 sent **Officialcrowns** a picture of a golden colored toilet paper roller rod (the rod in the center of a toilet paper holder) and ask **Officialcrowns** if that would work. **Officialcrowns** responded affirmatively. **Officialcrowns** tells V1 the video has to be 1 minute and 40 seconds and it has to go in as much as V1 can do. V1 sent a file of herself naked from the waist down. V1 is crouching down putting a portion of the golden roller rod in her vagina. V1 asks if it is good and that it is the only one she is doing. **Officialcrowns** responds, "You don't make the rules.. but you did just fine (V1).. good job!!" During the chat **Officialcrowns** tells V1 she lives in California "where the headquarters is located" and V1 responds that she lives in Oregon.

c. On August 10, 2018, **Officialcrowns** tells V1 to get her crop top on and her "knickers". The subject tells V1 she is going to "floss" (Floss is in reference to a type of dance move in which the arms and hips swing from side to side) for 30 seconds with them on and smile really big. V1 responds "Ok" and sends a video to **Officialcrowns** of herself doing a dance with her underwear and crop top on. Later in the conversation, **Officialcrowns** tells V1 to now "floss" with no "knickers". V1 sends a video where she is doing the same dance as before only with no underwear bottoms on and she bends down towards the camera and smiles.

d. V1 asks **Officialcrowns**, "Are we done for the day?" **Officialcrowns** responds, "Almost done". **Officialcrowns** then tells V1 to turn around and sit on the floor with her back to the camera, arching her back, and no underwear. V1 sends a photo of herself on her knees, buttocks towards the camera but resting upon her feet, head turned over her left shoulder and smiling back at the camera. **Officialcrowns** continues to instruct V1 and she sends two additional videos where she is posing in a similar manner. After sending the images/videos, V1 would ask **Officialcrowns** if the files were ok or good. V1 also asked if she was done taking photos and videos by saying, "Good for the day?" and "Are we good for the night?" After the last video is sent then **Officialcrowns** tells V1, "Tonight you are done…"

e. On August 12, 2018, V1 tells **Officialcrowns** "We have to go fast… Because I want to go to bed soon." **Officialcrowns** instructs V1 to squat without "knickers on", and she is going to push her hips back and forth while she rubs her "nunny" with her fingers on her "clit part". **Officialcrowns** also tells her to, "Go in circles with your fingers and moan quietly… then open it up at the end and hold it open." V1 sends a video as instructed, rocking her hips back and forth, masturbating and moaning and then holding her labia apart at the end. **Officialcrowns** then instructs V1 to lay on her back this time with her knees up by her sides and scoot up close to the camera. V1 does as instructed with the camera up close to her crotch area. In the video V1 masturbates and then leans forward to turn off the video.

f. **Officialcrowns** asks V1 if it felt good and she responds, "I don't really know" and "kind of". **Officialcrowns** tells V1 it will start to feel good after she does it long enough. Then **Officialcrowns** instructs her to lay on her back again like before and instead of circular motions, s/he tell her to go up and down her "nunny" and hold it open longer at the end. Then after that she will want to open her "bottom hole" too and to try to open it up really far. V1 send

a video, does as instructed and at the end she holds her labia apart and pulls her buttocks apart to show her anus.

g. On August 14, 2018, **Officialcrowns** started a chat with V1. **Officialcrowns** asks V1 to send her/him screen shots of her applications on her device including Facebook, Twitter, Instagram, YouTube, Snapchat, Musical.ly/tiktoc, and Funimate. V1 responded that she does not have those apps. The subject asks V1 how she stays in contact with her friends at school and at swimming. V1 states her friends do not have phones and only talks to them at school. V1 send the subject screenshots of her phone showing the apps. The subject also requested V1's email "in case Kik messes up." Later in the conversation V1 sends the subject her email address. **Officialcrowns** asks V1 what is her real age and V1 responded "10 all most 11."

h. On a chat that started on August 19, 2018, **Officialcrowns** advises V1 the "program is changing" and tells her that because school is starting she is going to have to start doing photos with partners on some days. **Officialcrowns** clarifies and tells V1 she is going to have to start doing photo while interacting with a partner, either another girl or another boy. V1 objects to this change and **Officialcrowns** tells her she will start doing them with her younger sister. V1 states she cannot do it with her sister and the subject later responds **Officialcrowns** will have to talk to "Musically". **Officialcrowns** convinces V1 to take a photo side-by-side with her sister. The girls are fully clothed. **Officialcrowns** tells V1 s/he will see if "musically" would like to have the sister take part in the photos.

i. On August 21, 2018, **Officialcrowns** sent V1 a photo to mimic, of a woman bent over at the waist, resting on a counter top with her buttocks towards the camera. The woman is wearing a top and underwear bottoms. V1 sent two photos to the subject of herself mimicking the older woman's pose. **Officialcrowns** also tells V1 to buy a jumbo size Sharpie as part of her

"school shopping". V1 sends a photo of a normal sized Sharpie. **Officialcrowns** does not explain what the Sharpie will be used for but tells V1 that it will be used the following day. V1 asks the subject "When will I do thing for points?" and **Officialcrowns** responds, "We have a bunch of time to earn points…"

Identification of Email and Social Media Accounts

14. Kik provided records on September 12, 2018 and October 17, 2018, for the **Officialcrowns** account pursuant to two separate subpoenas. The second subpoena was for updated IP addresses used by **Officialcrowns** to access Kik. The records showed the first and last name on the account was, ":sparkles:Official Moderator:sparkles:", and the email address listed was gjxicjcidthfufwictfsjppp@gmail.com. Information provided by Internet Service Providers for the IP addresses showed the internet was accessed by **Officialcrowns** in the Greensboro, North Carolina area when communicating with V1.

15. On September 10, 2018, I accessed and reviewed the email account belonging to V1 that she had given to **Officialcrowns** on or about August 14, 2018 through Kik. After V1 stopped communicating with **Officialcrowns** on Kik, a person unknown to V1, emailed her on August 30, 2018 from the email address **tager**dude25@gmail.com. The email states, "… you gotta respond soon or they will sell your stuff.. please remain active so I can help you." Information provided pursuant to a subpoena by the Google LLC for email account **tagerdude25@gmail.com** revealed several IP addresses used by the account. Information provided pursuant to a subpoena by the Internet Service Provider for one of the IP addresses used came back to an address in Gaston, South Carolina.

16. During the review of V1's email account, a second email was found from someone purported to be "Jessica Mills", a person unknown to V1, from email

Jessicamillsmoderator@outlook.com. The email, sent on September 2, 2018, from Mills stated, "We are having trouble getting in contact with you about finishing the program. Would you like to finish? Or would you like to start having your subscribers contact you again?" Information provided pursuant to a subpoena showed that the email account had been created on September 2, 2018 and the name on the account was "Jessica Mills."

17. An open source search for people associated with the Gaston, South Carolina address revealed **Andrew Thomas Tager**, date of birth XX/XX/1990, to be one of the people possibly associated with the address. A review of records with the Department of Motor Vehicles (DMV) for South Carolina and North Carolina conducted for **Tager** showed he had been issued a driver's license in both states. North Carolina issued the most recent driver's license for **Tager** on November 2016 and listed a Greensboro, North Carolina address.

18. An open source search was conducted for social media accounts belonging to **Tager**. An Instagram account under the username "**atagerofficial**" appeared to belong to **Tager**. The profile picture on the account looked like the same person in **Tager**'s DMV photos. The account had several pictures that were available for public view that featured **Tager** in them. Information provided pursuant to a subpoena for Instagram records showed the name listed on the account to be "**Andrew Tager**". The records showed the email address registered to the account was **tager**dude24@gmail.com. Records also showed the time and date IP addresses were used to log into the Instagram account. On September 8, 2018, the **atagerofficial** account logged in using IP address 174.255.130.57 at 13:45:30 UTC. A review of Kik records for **Officialcrowns** showed the same IP address, 174.255.130.57, was used on September 8, 2018 at 14:18:29 UTC. Verizon Wireless is the Internet Service Provider for IP address 174.255.130.57.

19. Starting on August 26, 2018, V1 received text messages from someone unknown

to her at phone number **(336) 314-6434**. The area code 336 is one of two area codes currently being used in the Greensboro, North Carolina area. The contents of the text messages included V1's name and "Hello". V1 did not respond to the text messages. The cell phone service provider with subscriber information was Tracfone Wireless, Inc. for phone number **(336) 314-6434**. Tracfone is a prepaid, no contract, reseller, mobile phone provider that does not require the user to provide their name to use their service. Subscriber records provided by Tracfone pursuant to a subpoena did not have the subscriber's name for the subject phone number **(336) 314-6434**. The records showed the account had been activated on May 24, 2017.

20. Verizon Wireless provided records pursuant to a subpoena for IP addresses used by **Officialcrowns** on Kik. The Verizon IP addresses were used by **Officialcrowns** between August 26, 2018 and September 12, 2018. The Verizon records showed phone number **(336) 314-6434** had been assigned the IP addresses during the times in question. Verizon is one of the wireless providers that Tracfone uses to offer their services as a reseller. Verizon maintained network connection records for phone number **(336) 314-6434**. The IP addresses submitted to Verizon included the IP address 174.255.130.57 that had been used at 13:45:30 UTC and 14:18:29 UTC by **atagerofficial** and **Officialcrowns** as noted previously.

21. A TikTok account under the username "**cherokeetager**" was found during the social media search and appeared to belong to **Tager**. The profile picture on the account appeared to be the same profile picture that was used in the Instagram account **atagerofficial**. Several videos on the account that were available for public view featured **Tager**. The profile also listed other social media accounts for **Tager**, Snapchat username "**cherokeetager**", and Instagram username "**atagerofficial**". Information provided pursuant to a subpoena for the TikTok **cherokeetager** account revealed the phone number associated with the account was

(336) 314-6434. Records also showed the account was created on June 19, 2017.

22. A subpoena for account information was served to Snapchat for user name **cherokeetager**. Snapchat records revealed the email for the account was **tager**dude28@gmail.com and the account was created on July 3, 2016. Records also showed several IP addresses used to login and logout of the account. The IP address 70.63.203.62 was used to login on August 21, 2018 at 16:25:14 UTC. IP Address 70.63.203.62 was compared to Kik records and revealed that the user of the **Officialcrowns** account had been on that IP address on August 21, 2018 at 16:23:24 UTC and 16:32:07 UTC. Information provided pursuant to a subpoena by the Internet Service Provider for the IP address 70.63.203.62 revealed that the IP address had been assigned to the Greensboro Public Library, located in North Carolina, since June 2016.

Google Records - tagerdude24@gmail.com

23. I reviewed the records provided by Google for the emails address tagerdude24@gmail.com. On January 5, 2018, tagerdude24@gmail.com, with the name listed as "gerald caulder", sent an email to tagerdude25@gmail.com. The subject line stated "Re: Ava's Crown Portfolio". The email stated that Ava had not been accepted for a "Crown" and it included a list of things she needed to complete to get into her portfolio. The list included that Ava needed to be trained by her Moderator "Musicalcrownpage" and she needed to improve her ability to listen and follow instructions from Musical.ly and her Moderator "Musicalcrownpage". The bottom of the email had the name listed as "Jarod Glazana", Musical.ly Director of Crown Distribution. The terms and subject matter discussed in the email was similar to the verbiage **Officialcrowns** used with chatting with V1. Some of the same terms used were "Program", "Crown," and "Moderator". The email also made to look like it was coming from an employee of

Musical.ly, like the Musical.ly employee Dianna that chatted with V1.

24. I found emails that indicated that the email address tagerdude24@gmail.com was controlled and used by **Tager**. For example, an email addressed to **Andrew Tager** that was from a credit card company and in another email there was a resume for **Andrew Tager** that contained a headshot picture of him. On an email dated March 21, 2019, tagerdude24@gmail.com, with the name listed as "gerald caulder", sent an email to tagerdude25@gmail.com. The email included an attached file that was a scanned copy of **Andrew Tager**'s, date of birth XX/XX/1990, North Carolina driver's license, number 000035129957. I believe the name "gerald caulder" was an alias for **Tager**.

Google Records - tagerdude25@gmail.com

25. I reviewed the records provided by Google for the emails address tagerdude25@gmail.com. In the records I found two video files of what I believe to be child pornography. On December 19, 2017, tagerdude25@gmail.com, with the name listed as Brian Zimmerman, sent an email to tagerdude24@gmail.com. The body of the email stated, "Toothbrush and shirt lift". The email had two video files attached. One video depicted what appears to be a minor female, approximately between 11 and 14 years of age, nude, exposing her chest and vagina. The minor female, multiple times, rapidly inserts and removes a toothbrush from her vagina. On a separate email also dated December 19, 2017, tagerdude25@gmail.com, with the name listed as Brian Zimmerman, sent an email to tagerdude24@gmail.com with the subject line, "From behind ass opening". The email contained a video file in which a minor female, approximately between 9 and 12 years of age, is nude from the waist down, spreading her buttocks, and exposing her vagina and anus to the camera.

26. On July 3, 2018, tagerdude25@gmail.com, with the name listed as Brian

Zimmerman, received an email from what appeared to be an adult female. The email contained a string of emails between the two dating back to May 2015. In one email, tagerdude25@gmail.com told the user that she could contact him on his Kik account, username **Officialcrowns**. As described previously, **Officialcrowns** was the same Kik account the subject used to chat with V1.

27. On August 30, 2018, tagerdude25@gmail.com, name listed Brian Zimmerman, sent an email with the subject line, "Your Program Status." The email states, "... you gotta respond soon or they will sell your stuff.. please remain active so I can help you." This email was the same email V1 received. I believe the name Brian Zimmerman is an Alias for **Tager**. In another email to **Tager** from his brother, his brother asks, "You still going by Brian Zimmerman? Lol You never explained that alias to me."

28. I found emails that indicated that the email address tagerdude25@gmail.com was controlled and used by **Tager**. On December 29, 2018, tagerdude25@gmail.com, now with the name listed as **Andrew Tager**, emailed an individual with the subject line, "**Andrew Tager**'s Resume." In the body of the email, tagerdude25@gmail.com states he is **Andrew**. It also states that he is looking for a career in the gaming industry and is signed "Kind Regards, **Andrew Tager**." Attached to the email was a file called "Resume_Andrew Tager.PDF." The resume had **Tager**'s phone number listed as **(336) 314-6434**.

TikTok Records – Cherokee

29. I reviewed TikTok records for the **cherokeetager** account which I believe was used by **Andrew Tager**. The profile picture on the account appeared to be **Tager**. During the review, I discovered that **cherokeetager** had contacted several other TikTok users that appeared to be minor females and told them about a "Crown Program". In one chat conversation between

cherokeetager and a user identified with ID number 6559335184284745734. **Cherokeetager** states that he is in a Crown Program that promotes his account directly and he gains more fans and likes. **Cherokeetager** told the other user to download the Kik app and let him know when it is downloaded so he can have "Jessica" contact them. **Cherokeetager** states that she, Jessica, sets up the rules. **Cherokeetager** told the user that he had to do exactly everything she was doing and that Jessica was very smart and she will take 100% care of her. **Cherokeetager** states, "I swear on my life, if you listen to Jessica, she will gain you ALOT of fans." Later **Cherokeetager** tells the user to get back on the Crown Program app and talk to Jessica. I reviewed the profile page of user ID 6559335184284745734 and she is a minor approximately between 10 and 12 years of age.

30. In another chat between between **Cherokeetager** and user ID 6626056930223931397, **Cherokeetager** tells the user that if she wants fans like him they need to get the Kik app. **Cherokeetager** tells the user the app is needed to talk to Jessica and describes her as a Moderator for TikTok Headquarters. The user states she can't download the app and **Cherokeetager** responds, "Ok then you don't get any fans and you don't get a Crown." I reviewed the profile page of user ID 6626056930223931397 and she is a minor approximately between 10 and 12 years of age.

High Point Police Department

31. I reviewed an incident report from the High Point Police Department, North Carolina, from June 2017 involving **Tager**. In the incident report, the complainant advised that her 12 year old daughter had been receiving inappropriate messages from **Tager**. The complainant alleged that **Tager** was texting her daughter using the app Snapchat. **Tager** told the minor female that he wanted to date her and her twin sister. **Tager** said he wanted them at the

same time "as package deal." **Tager** told the minor female not to tell her mom and not save the messages on Snapchat. **Tager** said he wanted to take the twins swimming and he would take the minor female's top off. Also, after the minor female stated she was a virgin, **Tager** stated, "you won't be after this, you're gonna love have sex with me." **Tager** was interviewed by detectives and he denied making any illegal or inappropriate conversations on any app with the minor females in the case. The local district attorney's office reviewed the case and declined to pursue charges in the matter.

Interview of V2

32. On April 2, 2019, V1's friend, V2, that told her about earning a "Crown", was interviewed by a child forensic interviewer in Oregon. Shortly after getting the Musical.ly app someone started following V2. The follower explained how she could earn a "crown" in Musical.ly and she needed to download the app Kik and add a person. V2 downloaded Kik and the person started asking for pictures. V2 was told if she did not send the picture they would hurt her family. V2 was nine years old and in fourth grade when she first started communicating with the person on Kik. Initially V2 said no to taking pictures. V2 then sent nude pictures and videos of herself to the person on Kik because she didn't want her family to get hurt. The videos included her dancing naked. The nude pictures included her squatting and showing her buttocks. The person would instruct V2 on how to pose. V2 took nude pictures of her whole body. V2 did not remember the user name for the person on Musically or Kik but she thought they were both something like "Get a crown now". The person on Kik told V2 that her name was Dianna and worked for Musically. V2 thought this person was the same person that had told V1 to send him photos and videos.

The Vic Apartments, Greensboro, North Carolina

33. I reviewed records for Snapchat account **cherokeetager**, the account associated with **Tager**. I found that in November 2018, **cherokeetager** told another user to download the Kik app so the user could talk to "Jessica" to get more fans and likes by doing the "program". **Tager** told the user Jessica's account on Kik was **Tiktokofficial**. On April 30, 2019, I reviewed records from Kik for the account that included IP address information. From March 31, 2019 to April 25, 2019, the account **cherokeetager** had only used one IP address, 174.111.194.27. The IP address was used by a Charter Communications customer. I had previously reviewed Charter Communications records for that IP address, which had also been used in October 2018 by **Officialcrowns**, and the service address came back to 707 Milton Street, Apt, 3N, Greensboro, North Carolina 27403. On May 1, 2019, I reviewed records from Charter Communications for the IP address 174.111.194.27 for use from March 31, 2019 to April 25, 2019 and confirmed it was still used at the same service address.

34. The address 707 Milton Street, Apt, 3N, Greensboro, North Carolina 27403 is located at The Vic Apartments. Lease records for the apartment showed that three females lease the apartment but **Tager** was not on the lease. I believe one of the females is in a relationship with **Tager**. On email account tagerdude24@gmail.com, **Tager** emailed the female at a similar email address that was provided for her by The Vic Apartments. In another email the tagerdude25@gmail.com account, **Tager** stated he was the boyfriend of the female by referencing her first name. It has not been confirmed if **Tager**'s primary residence is 707 Milton Street, Apt, 3N, Greensboro, North Carolina 27403.

Conclusion

35. Based on the above information, I have probable cause to believe, and do believe,

that **Tager** violated Title 18, United States Code, § 2251(a), involving the production of child pornography, and Title 18, United States Code, § 2252A, involving the transportation, receipt, and possession of child pornography. I therefore request that the Court issue the requested criminal complaint and arrest warrant.

36. Prior to being submitted to the Court, this affidavit and the requested arrest warrant were all reviewed by Assistant United States Attorney (AUSA) Amy Potter, and AUSA Potter advised me that in her opinion the affidavit is legally and factually sufficient to establish probable cause to support the issuance of the requested complaint and warrant.

Miguel A. Perez
Special Agent, Federal Bureau of Investigation

Subscribed and Sworn to before me this 2 day of May, 2019.

Thomas Coffin
United States Magistrate Judge

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

District of Oregon

Eugene Division

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Apple iPhone 5S cellular telephone, model number A1453, with serial number 352029066888465, currently located at 9109 NE Cascades Pkwy, Portland, OR 97220

Case No. 6:20-mc-30

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of Oregon
(identify the person or describe the property to be searched and give its location):

Apple iPhone 5S cellular telephone, model number A1453, with serial number 352029066888465, currently located at 9109 NE Cascades Pkwy, Portland, OR 97220 as described in Attachment A hereto.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

YOU ARE COMMANDED to execute this warrant on or before 1/24/2020 *(not to exceed 14 days)*
☐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Mustafa T. Kasubhai, United States Magistrate Judge.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 11:03 am, 1/10/2020

City and state: Eugene, Oregon

Mustafa T. Kasubhai, United States Magistrate Judge
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
6:20-mc-30	1/21/2020 1:00 pm	None

Inventory made in the presence of :
None

Inventory of the property taken and name of any person(s) seized:

IPhone 5s, Model # A1453, Serial: 352029066888465.

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 1/21/2020

Miguel A. Perez
Executing officer's signature

Miguel A. Perez, Special Agent
Printed name and title

ATTACHMENT A

Property to Be Searched

The property to be searched is an Apple iPhone 5S cellular telephone, model number A1453, with serial number 352029066888465 and is currently located on the premises of the Federal Bureau of Investigation at 9109 NE Cascades Parkway, Portland, Oregon 97220.

ATTACHMENT B

Items to Be Seized

1. All records on the Device described in Attachment A that relate to violations of Title 18, United States Code, §§ 2251(a) and 2252A, involving the production of child pornography and transportation, distribution, receipt, and possession of child pornography, and involves Andrew Thomas Tager since June 1, 2015, including:

a. Any and all records, documents, or materials, including correspondence, that pertain to the production, possession, receipt, transportation, or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in as defined in Title 18, United States Code, Section 2256.

b. All originals and copies of visual depictions of minors engaged in sexually explicit conduct, as defined in as defined in Title 18, United States Code, Section 2256.

c. Any and all motion pictures or digital video clips of visual depictions of minors engaged in sexually explicit conduct, as defined in as defined in Title 18, United States Code, Section 2256, video recordings which are self-produced and pertain to sexually explicit images of minors; or video recordings of minors which may assist in the location of minor victims of child exploitation or child abuse;

d. Any and all records, documents, or materials which include offers to transmit, through interstate commerce by any means, any visual depiction of a minor engaged in sexually explicit conduct, as defined in as defined in Title 18, United States Code, Section 2256.

e. Any and all records, documents, or materials relating to the production,

reproduction, receipt, shipment, trades, purchases, or transactions of any kind involving the transmission, through interstate commerce, of any visual depiction of a minor engaged in sexually explicit conduct, as defined in as defined in Title 18, United States Code, Section 2256.

f. Any and all records, documents, or materials naming or identifying minors visually depicted while engaging in sexually explicit conduct, as defined in as defined in Title 18, United States Code, Section 2256.

g. Any records of Internet usage, including records containing screen names, user names, and e-mail addresses, and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, and e-mail messages..

Search Procedure

5. The examination of the Device may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

6. The initial examination of the Device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of

the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

7. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Device or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

8. If an examination is conducted, and it is determined that the Device does not contain any data falling within the ambit of the warrant, the government will return the Device to its owner within a reasonable period of time following the search and will seal any image of the Device, absent further authorization from the Court.

9. The government may retain the Device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Device and/or the data contained therein.

10. The government will retain a forensic image of the Device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.